## REMARKS

In Response to applicant's prior amendment the examiner stated:

> **2. Claim 2, which is "currently amended", is not presented with marking(s) to indicate the change(s) that have been made relative to the immediate prior version. Appropriate correction is required.**
>
> **3. Claim 11, which has been changed, but is not indicated as being "currently amended". Appropriate correction is required.**
>
> **4. The Applicant has indicated the paragraph beginning at page 4, line 24 to be replaced with the amended paragraph filed 07/28/2005. However, the paragraph to be replaced begins at page 5, line 3 of the Specification. Appropriate correction is required.**

In the prior response claim 2 was not intended to be amended. Applicant had the incorrect status identifier.

In claim 11 the amendment was intended and has been incorporated into the amendments made herein.

The correct page and line number has been provided for the replacement paragraph in the specification.

The examiner rejected Claims 1-3, 5-8, 10-1 3, 15, 17-1 9 and 21 -22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Mansfield ("Towards Trapping Wily Intruders in the Large") in view of Mell et al ("Mobile Agent Attack Resistant Distributed Hierarchical Intrusion Detection Systems")..

Claim 1

With regard to claim 1 applicant stands by the arguments of record, namely, that Claim 1 is allowable since the references neither describe nor suggest *** a computing device that cpacket traffic over a network, and which accumulates and collects statistical information about the packet traffic *** and a port to link the data collector over a redundant network that does not carry the packet traffic to deliver the accumulated and collected statistical *** . Accordingly, claim 1 is allowable over the references for the reasons of record.

Claim 2

Applicant has amended claim 2 to call for ... instructions to collect statistical information pertaining to network packets received by the data collector. Claim 2 also requires that the data collector include a port to link the data collector over a redundant network that does not carry the packet traffic to deliver collected statistical data about the network packets to a central control center upon demand by the central control center.

The examiner contends that:

> **Regarding claims 1-3, 11 and 21, Mansfield discloses a method for a data collector to collect data from sampled network traffic comprising: sampling packet traffic over a network and generating statistical information about the packet traffic on the network (Section 3, Detection of Intrusions from traffic-flow signatures; Section 5, Implementations and Results); parsing the information in the sampled packets and maintaining the information in a log (Section 3, Detection of Intrusions from traffic-flow signatures); and delivering the generated statistics over a network to a central control center (Section 5, Implementations and Results; Section 3.1, Traffic-flow signature). Mansfield does not disclose utilizing a redundant network that does not carry the packet traffic to deliver the generated statistics to a central control center. Mell discloses utilizing a separate and protected network for communications between data collectors and a control center (Section 2.0, Background on Distributed Hierarchical IDSs; Section 3.0, Vulnerable Systems). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the Mansfield method to utilize a separate and protected network for communications between the data collector and the control center, as taught by Mell, so that the data collector would not be isolated in the event an attacker floods the communication channel on which the data collector is residing.**

The examiner contentions regarding Mansfield are incorrect. Mansfield fails to suggest "sampling packet traffic over a network and generating statistical information about the packet traffic on the network or parsing the information in the sampled packets and maintaining the information in a log.

Mansfield also fails to suggest delivering the generated statistics over a network to a central control center at Section 5, Implementations and Results, Section 3.1, Traffic-flow signature or elsewhere.

Mansfield Section 5, Implementations and Results is reproduced below:

> **The traffic monitoring is carried out using agents which watch all the traffic but process only the suspicious packets. The agents can be accessed, queried and configured using the standard SNMP management protocol. The Security**

**Manager system is alerted on the detection of potential attempts. The Security Manager uses the network configuration information to trap and/or track-down the intruder. The communication between the different Manager's and the agents is carried out using the standard SNMP management protocol. The communication utilizes the security features provided in the SNMP framework viz. authenticity confidentiality, integrity, reliability. The asynchronous alerts are communicated using Inform requests. The message conveyed contains a list of managed objects describing the event that has been detected. The prototype is currently under evaluation.**

According to Mansfield the agents, process only suspicious packets and these agents are queried using SNMP. According to Mansfield in Section 3, Mansfield uses the traffic monitors to collect the relevant packet count and the NMS (which is not defined or enabled in Mansfield) correlates relevant packet count information from each link. See Mansfield 3.1 reproduced below.

**3.1 Traffic flow signatures**

**The basic concept of signature-based traffic tracing is shown in Fig.4. The traffic monitor 'collects the relevant packet count information from each link, which connects the sites. The NMS compares the monitored traffic pattern, and correlates them. The correlated chain of patterns indicates the path of (probably spoofed) traffic-flow. It should be noted that the information used is packet count only, neither packet capture nor analysis is needed.**

However, Mansfield does not describe an actual system, but rather an experiment that was set up on a medium sized campus network (Mansfield p. 2) with two network probes to measure ICMP network response packets. Apparently offline, these measurements were correlated to each over different times. However, in no instance did Mansfield describe or suggest ... instructions to cause the computing device to collect statistical information pertaining to network packets ...with the data collector including a port to link the data collector over a redundant network that does not carry the packet traffic to deliver collected statistical data about the network packets to a central control center upon demand by the central control center, as recited in claim 2.

The examiner acknowledges that Mansfield is deficient in failing to suggest at least this later feature that the data collector includes: "a port to link the data collectors over a redundant network that does not carry the packet traffic to deliver collected statistical data about the network packets to a central control center upon demand by the central control center."

The examiner relies on Mell to teach this feature. As argued of record, Mell discloses mobile agent attack resistant distributed hierarchical intrusion detection systems. According to Mell, a solution to the problem related to the vulnerability of distributed intrusion detection systems is to cast the internal nodes in the system hierarchy as mobile agents. These mobile agents randomly move around the network such that an attacker can not locate their position. While, Mell in (Section 3.0, Vulnerable Systems) discloses: "One solution to this problem is to provide IDSs a separate and protected communication channel for their operation. This solution works well but is very costly, as separate cables must be run for the IDS system."

In Applicant's prior response, Applicant argued that the motivation offered was insufficient in view of the reference clearly teaching away from the feature. In response the examiner argued that:

> **It is well known in the art of network security that there often is more than one solution to a security problem and that a solution is selected based on a particular system's security requirement, performance and/or cost. Therefore, for a system that does not tolerate security compromises and where cost is not an issue, it would be obvious to one of ordinary skill in the art to select the known solution of using a separate communication channel. (Office action page**

Despite the reference obviously teaching away from that solution, the examiner's motivation fails to suggest a basis upon which one of ordinary skill in the art would modify Mansfield. Mell does not elaborate on what "separate protected communication channels for IDS nodes" are. Claim 2 calls for "a port to link the data collector over a redundant network that does not carry the packet traffic to deliver the accumulated and collected statistical information *** ." The examiner cannot argue that Mell meets this feature of claim 2. Merely providing a separate channel does not guarantee that the data collector sends the statistical information over "a redundant network that does not carry the packet traffic." Rather, Mell does not suggest much less describe that the communication channel would not use portions of the network monitored by the IDS systems.

It would not be suggested to one of ordinary skill in the art therefore, to modify Mansfield with Mell to provide the claimed feature of a port to link the data collectors over a redundant network that does not carry the packet traffic to deliver collected statistical data about

the network packets to a central control center upon demand by the central control center, because Mell clearly teaches away from that feature and fails to describe or suggest the feature as now claimed.

Accordingly, the motivation to modify Mansfield to include a redundant network that does not carry the packet traffic to deliver the accumulated and collected statistical information about the network packet traffic to a central control center is not present. Therefore, claim 2 is allowable over the references.

Claims 3, 5-8, and 10 depend directly or indirectly on claim 2 and are allowable with claim 2.

Claims 11-13, 15, 17-19 and 21-22 are also allowable because they each include a similar limitation of a port to link the data collectors over a redundant network a redundant network that does not carry the packet traffic to deliver collected statistical data about the network packets to a central control center.

The examiner rejected Claim 4 under 35 U.S.C. 103(a) as being unpatentable over Stallings in view of Mell and official notice.

Claim 4, as amended, is allowable over the cited references. Mell does not suggest much less disclose "a dedicated line" in (Section 3.0, Vulnerable Systems).

Mell also does not disclose that the dedicated line is a leased telephone line. The Examiner took Official Notice that using a "leased line" as a dedicated line is well known in the art. Applicant has amended claim 4 to limit the leased line to a "leased telephone line." In view of the discussion above, it would not be obvious to use a leased line or a telephone line or a leased telephone line.

The examiner rejected Claim 14 under 35 U.S.C. 103(a) as being unpatentable over Mansfield in view of Mell, as applied to claim 13, and further in view of Zait et al., U.S. Patent 6,665,684.

Claim 14 further limits the method of claim 13 by dividing the traffic flow into buckets that track counts of how many packets a data collector or gateway examines for a given

parameter and adjusting the number of buckets ... by combining several buckets into fewer buckets or dividing a bucket into more buckets.

The examiner contends that Mansfield teaches "dividing the traffic flow and using memory spaces to track counts of how many packets a data collector examines for a given parameter (p5, 1st par). ..." In this passage cited by the examiner, Mansfield is merely discussing setting thresholds to see how many related packets are received in order to catch low rate scanner attacks. Mansfield neither describes nor suggests to divide the traffic flow into buckets that track counts of how many packets a data collector or gateway examines for a given parameter. The examiner admits that Mansfield does not disclose: "adjusting the number of buckets ... by combining several buckets into fewer buckets or dividing a bucket into more buckets" relies on Zait for this teaching.

However, Zait neither describes nor suggests dividing the traffic flow into buckets nor adjusting the number of buckets ... by combining several buckets into fewer buckets or dividing a bucket into more buckets. Zait is directed to database table partitioning. Zait discusses three types of partitions "hash-based partitioning and range-based partitioning" (Col. 4 lines 11-12) and a composite partition. (Col. 4 line 10) Zait describes that: "with range-based partitioning, it becomes necessary to add new partitions when newly arriving rows have partition key values that fall outside the ranges of existing partitions." (Col. 4 lines 13-16) Zait describes that: "... all partition key values fall within existing partitions of a hash-partitioned table. However, it may be desirable to add new partitions to a hash-partitioned table, for example, to spread the data over a greater number of devices." (Col. 4 lines 22-26) Zait describes a composite technique of range and hash based partitions.

The partitions that Zait discusses are records in a table, e.g., to divide a table of records according to some criteria to make database management easier, e.g., improving access to objects (Col. 3 lines 44-45).

Neither Zait nor Mansfield nor Mell suggest the desirability of dividing the traffic flow into buckets that track counts of packets examined for a given parameter and adjusting the number of buckets ... by combining several buckets into fewer buckets or dividing a bucket into

more buckets. Neither appreciates the problem of an attack that exploits memory space. Zait teaches database management, and is not concerned with attacks that exploit memory space. Mansfield although addressing techniques to address attacks does not recognize the problem of attacks that exploit memory space. Accordingly, claim 14 is allowable over the art, since the combination of references do not suggest the claimed elements and further that there is no suggestion to combine the references.

The examiner rejected Claim 16 under 35 U.S.C. 103(a) as being unpatentable over Mansfield in view of Mell as applied to claim 15, and further in view of Roesch "Snort-Lightweight Intrusion Detection for Networks."

Claim 16 limits claim 15 by requiring that the layer 3-7 analysis involves monitoring network traffic for unusual levels of IP fragmentation, or fragmented IP packets with bad or overlapping fragment offsets.

Roesch describes reassembly of fragments to allow full payload decoding and alerting in the presence of packet fragments smaller than a predetermined size. Claim 16 recites monitoring for unusual levels of IP fragmentation (that is, more fragmented packets, of any size, than would normally be expect on the network), and detection of fragments with invalid or overlapping fragment offsets. As such, Roesch neither describes nor suggests the features of claim 16.

The examiner rejected Claim 20 under 35 U.S.C. 103(a) as being unpatentable over Mansfield in view of Mell as applied to claim 15, and further in view of Eichstaedt et al., U.S. Patent 6,662,230.

Claim 20 further limits claim 15 by reciting that the layer 3-7 analysis includes monitoring network traffic for an indication of a frequency of re-load requests that are sustained at a rate higher than plausible for a human user over a persistent HTTP connection. The examiner admits that neither Mansfield nor Mell address this feature, and instead relies on Eichstaedt. Eichstaedt pertains to web robots or web-crawlers that obtain documents from a web server.

Initially, applicant notes that claim 20 is directed to a method of collecting data from sampled network traffic, not collecting web pages from a server as taught by Eichstaedt. Eichstaedt teaches to allow a server to limit access to client systems (Col. 6, lines 21-39). Eichstaedt does not suggest monitoring network traffic for an indication of a frequency of reload requests that are sustained at a rate higher than plausible for a human user over a persistent HTTP connection. Eichstaedt also does not provide any motivation or solution suitable in the context of Mansfield and Mell or Applicant's claim 20. While Eichstaedt teaches to limit access to client systems (Col. 6, lines 21-39), such a solution is of no import to an intrusion detection system, as taught by the references. Accordingly, whether taken separately or in combination there is no suggestion in Eichstaedt nor the other cited art of monitoring network traffic for an indication of a frequency of reload requests that are sustained at a rate higher than plausible for a human user over a persistent HTTP connection. Therefore, claim 20 is also allowable.

The examiner rejected Claims 1-13 and 21 under 35 U.S.C. 103(a) as being unpatentable over Stallings "Cryptography and Network Security: Principles and Practice," in view of Mell et al.

Claim 1 is allowable over these references for the reasons of record.

Claim 2, as amended recites ... instructions to collect statistical information pertaining to network packets received by the data collector, ...and ... the data collector further comprises a port to link the data collectors over a redundant network that does not carry the packet traffic to deliver collected statistical data about the network packets to a central control center upon demand by the central control center. The combination of these features is neither described nor suggested by Stallings in view of Mell et al.

The examiner contends that Stallings teaches "sampling the network traffic and generating statistics about the network flow," and acknowledges that "Stallings does not disclose utilizing a hardened, redundant network. The examiner relies on Mell to teach this feature, using the same motivation in the rejection based on Mansfield and Mell.

Stallings is directed to intrusion detection systems. Stallings has no relevant teachings related to statistical data. In Stallings, so called audit collection process produces audit records

that are filtered to retain records of interest. Stallings does not suggest of instructions to perform sampling and statistic collection of data pertaining to network packets nor a redundant network that does not carry the packet traffic to deliver the accumulated and collected statistical information about the network packet traffic *** , and thus does not cure the deficiencies of Mell.

Mell discloses mobile agent attack resistant distributed hierarchical intrusion detection systems. According to Mell, a solution to the problem related to the vulnerability of distributed intrusion detection systems is to cast the internal nodes in the system hierarchy as mobile agents, as discussed above.

While, Mell (Section 3.0, Vulnerable Systems) discloses: "One solution to this problem is to provide IDSs a separate and protected communication channel for their operation. This solution works well but is very costly, as separate cables must be run for the IDS system." again, as discussed above, this disclosure is insufficient to suggest the claimed feature.

In addressing Applicant's prior response the examiner argued that:

> **It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the Stallings method to utilize a separate and protected network for communications between the data collector and the control center, as taught by Mell, so that the data collector would not be isolated in the event an attacker floods the communication channel on which the data collector is residing.**

Despite the obvious teaching away from that solution expressed in the reference itself, this motivation fails to suggest a basis upon which one of ordinary skill in the art would modify Stallings. Mell does not elaborate on what "separate protected communication channels for IDS nodes" are. Claim 2 now calls for "a port to link the data collector over a redundant network that does not carry the packet traffic to deliver the accumulated and collected statistical information *** ." The examiner cannot argue that Mell meets this feature of claim 2. Merely providing a separate channel does not guarantee that the data collector sends the statistical information over "a redundant network that does not carry the packet traffic." Rather, Mell does not suggest much less describe that the communication channel would not use portions of the network monitored by the IDS systems.

It would not be suggested to one of ordinary skill in the art therefore, to modify Stallings with Mell to provide the claimed feature of a port to link the data collectors over a redundant network that does not carry the packet traffic to deliver collected statistical data about the network packets to a central control center upon demand by the central control center, because Mell clearly teaches away from that feature and fails to describe or suggest the feature as claimed.

Accordingly, the motivation to modify Mansfield to include a redundant network that does not carry the packet traffic to deliver the accumulated and collected statistical information about the network packet traffic to a central control center is not present. Therefore, claim 2 is allowable over the references.

Claims 3-13 and 21 are allowable for analogous reasons over these references.

The prior art not relied on is seen as neither describing nor suggesting applicant's claims whether taken separately or in combination with the art of record.

Enclosed is a **$60** check for the Petition for Extension of Time fee. Please apply any other charges or credits to deposit account 06-1050.

Respectfully submitted,

Date: 2/1/06

Denis G. Maloney
Reg. No. 29,670

Fish & Richardson P.C.
225 Franklin Street
Boston, MA 02110
Telephone: (617) 542-5070
Facsimile: (617) 542-8906